SANDBOXAQ™

Cryptographic Posture and PQC Readiness

What Every CISO Needs to Know

James Howe
Head of Cryptography

https://www.linkedin.com/in/jameshowe1729/
james.howe@sandboxaq.com

Presentation outline

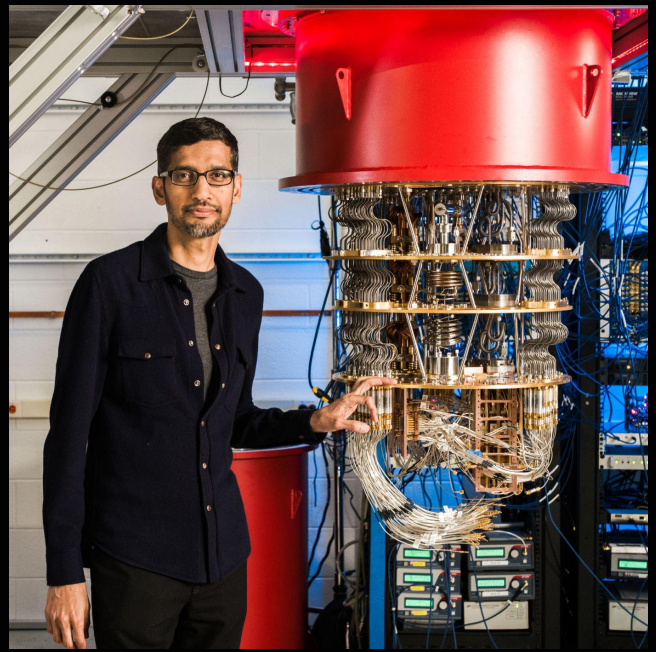
1. **Quantum Computers**
   And its threat to current cryptography standards.
2. **Post-Quantum Cryptography (PQC)**
   The new standards dealing with this existential threat.
3. **The PQC Challenge**
   Understanding enterprise complexities.
4. **A New Approach**
   Integrated discovery and management, utilizing existing infrastructure.

01 The Threat of Quantum Computers

Quantum Computers

Quantum computers are here:

- **Unlocking New Capabilities:** Solves problems intractable for classical systems, accelerating innovation in drug discovery, materials, and AI.
- **Transforming Industries:** Optimizes logistics, finance, and R&D, driving significant business advantages.
- **Emerging Threat to Security:** Undermines foundational algorithms (e.g., RSA) securing current data and communications.
- **Strategic Imperative:** Proactive defense against quantum threats is vital for long-term security and competitive edge.



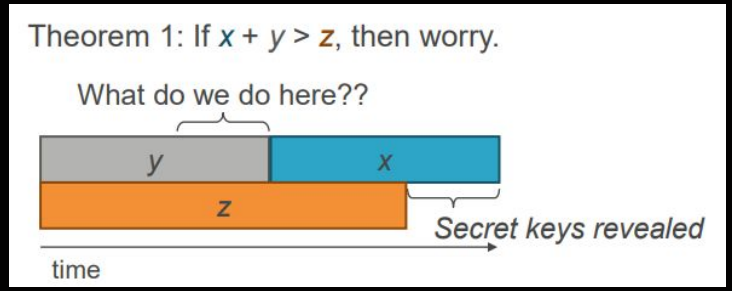
Store Now, Decrypt Later (SNDL)

Today

Today's sensitive data can still be value in the future, when it can be decrypted with quantum computers

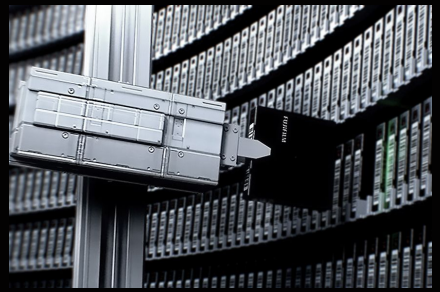
Tomorrow

Companies and infrastructures need to adopt measures against quantum computers now, and there are already mechanisms for that.



Mosca's inequality theorem

Storage



Data retrieval

Quantum processing

Decrypted message

When is doomsday?

10-30 years

Today — 2035 — 2055

RSA-2048 broken with probability 50-99%

Jul. 2017 — 51 qubits — HARVARD UNIVERSITY

Feb. 2018 — 72 qubits — Google

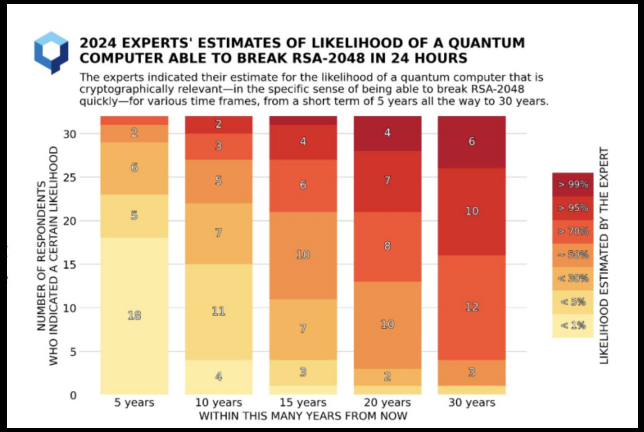
Sep. 2019 — "Quantum supremacy" — Google

Dec. 2024 — 105 qubits — Google

Other companies building quantum computers include:

- Amazon
- IBM
- Microsoft
- and many others

Global Risk Institute Quantum Threat Timeline Report 2024
https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/



SANDBOXAQ™

Quantum Threat to RSA-2048

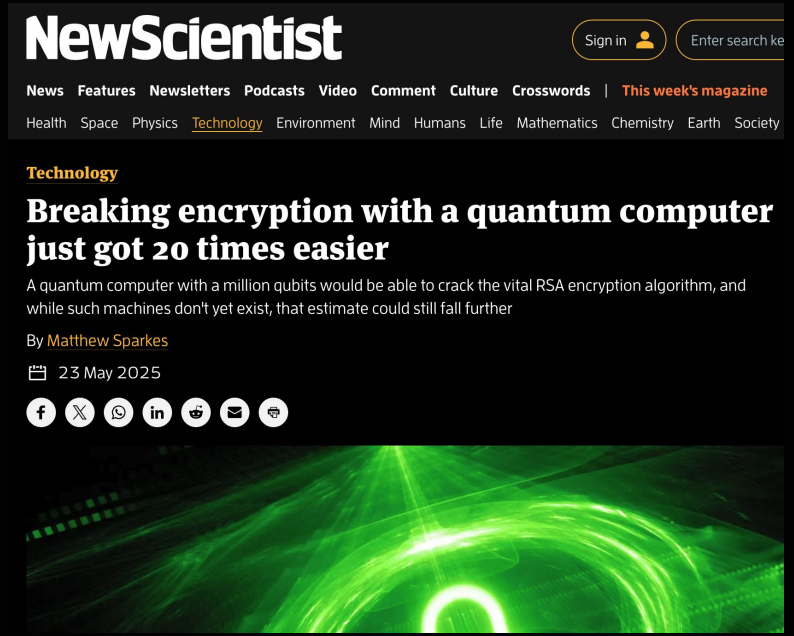
Recent Research (May 2025): Breaking RSA-2048 encryption is now estimated to be 20 times easier than previously thought.

Logical Qubit Comparison (RSA-2048):

- Current Best Estimate: 1,399 logical qubits
- Previous Record (2024): 1,730 logical qubits

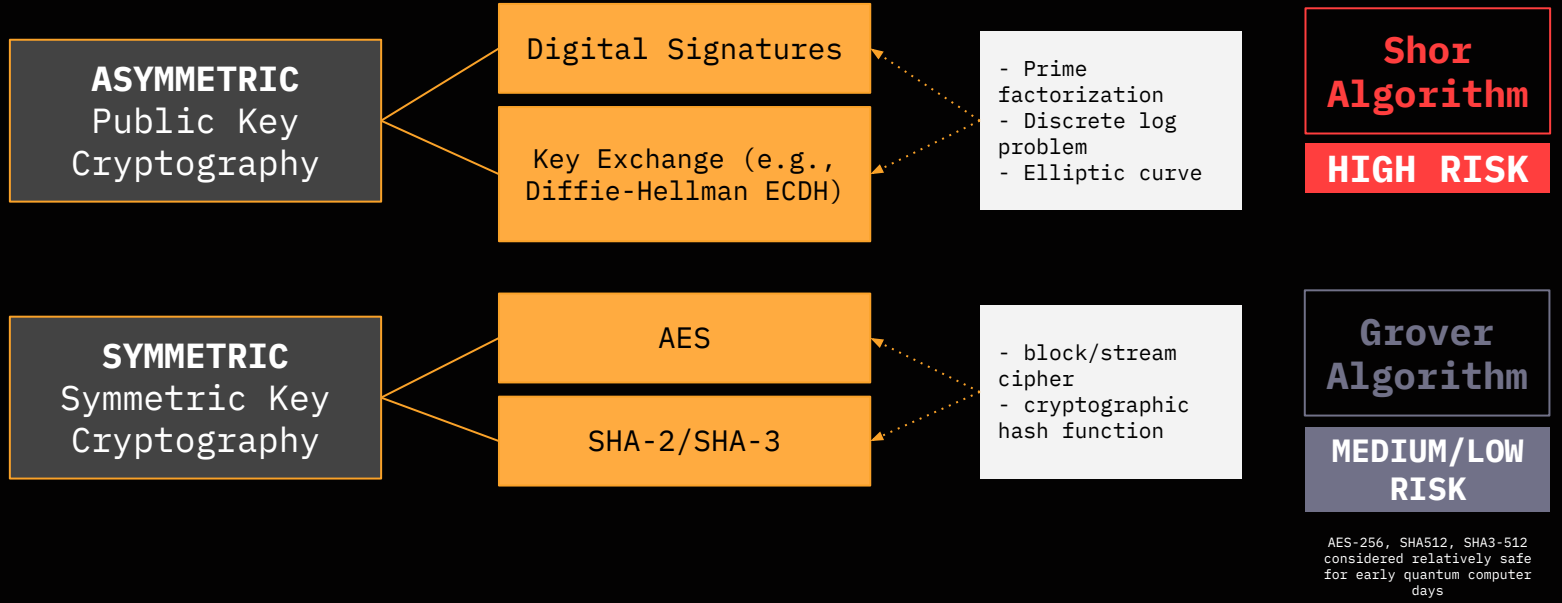
Impact: Continued advancements are driving down resource requirements for quantum attacks, accelerating the timeline for quantum-safe cryptography transition planning.

Action: Continue to prioritize and accelerate the transition to quantum-resistant cryptosystems.



02 Post-Quantum Cryptography

Cryptography at risk



Quantum Algorithms:
The good, the bad, and the ugly

	The good	The bad	The ugly
SHOR'S ALGORITHM	gives exponential speed-up for factoring integers.	requires quantum hardware, i.e. a LFT quantum computer.	combining these breaks current public-key standards.
GROVER'S ALGORITHM	gives quadratic speed-up for unstructured searching.	requires quantum hardware, i.e. a LFT quantum computer.	combining these means symmetric-key security is halved.

New Public-Key Cryptography Standards

A method for establishing a shared key.

Basically, what we want is:

A method for authentication.

NIST PQC Standardization Process

Submissions	Accepted R1	Accepted R2	Accepted R3	Accepted R4	Standardized
82	69	26	15	4	5

Apr 2016
NISTIR 8105 Report

Dec 2016
Formal Call for Proposal

Nov 2017
Deadline for Submissions

Dec 2017
1st Round candidates announced

Apr 2018
1st NIST PQC Standardization Workshop

Jan 2019
2nd Round candidates announced

Aug 2019
2nd NIST PQC Standardization Workshop

July 2020
3rd Round Schemes announced

Q2/Q3 2021
3rd NIST PQC Standardization Workshop

July 2022
Algorithms to standardize and 4th round schemes announced

Jan 2023
New Standards Process for more Signatures.

Oct 2024
SandboxAQ candidate, SDitH, selected for round 2

March 2025
SandboxAQ candidate, HQC, selected for KEM standard

SANDBOXAQ™

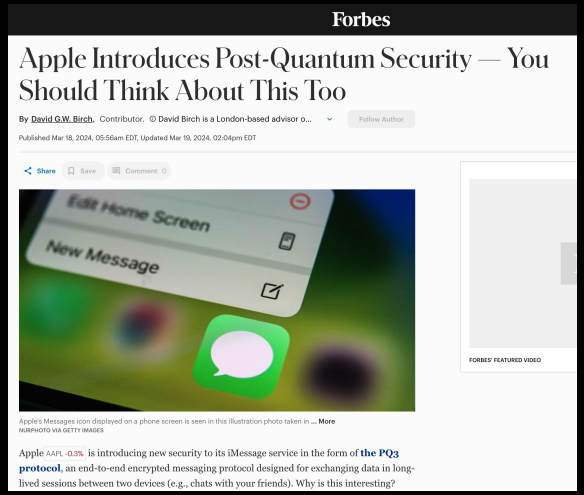
NIST PQC Standardization Process

Submissions	Accepted R1	Accepted R2	Accepted R3	Accepted R4	Standardized
82	69	26	15	4	5

PQC standards to-date:

- **Key Encapsulation Mechanisms / Public-Key Encryption:**
  - ML-KEM (FIPS 203): Primary PQC standard for general encryption.
    - Adopted in iMessage, Signal, and in TLS deployments.
  - HQC: alternative to ML-KEM, based on coding theory.
  - Unlikely more coming…

- **Digital Signature Algorithm (DSA):**
  - ML-DSA (FIPS 204): Primary standard for digital signatures.
  - SLH-DSA (FIPS 205): based on hash functions
  - Falcon: also lattice-based like ML-KEM and ML-DSA
  - More coming…



Forbes

Apple Introduces Post-Quantum Security — You Should Think About This Too

By David G.W. Birch, Contributor. © David Birch is a London-based advisor o...

Published Mar 18, 2024, 05:56am EDT, Updated Mar 19, 2024, 02:04pm EDT

Share Save Comment

Apple's Messages icon displayed on a phone screen is seen in this illustration photo taken in ... More

NURPHOTO VIA GETTY IMAGES

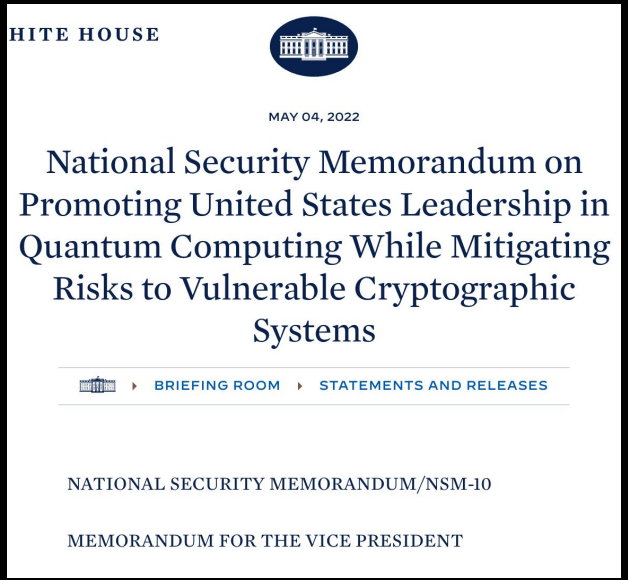
Apple AAPL -0.3% is introducing new security to its iMessage service in the form of **the PQ3 protocol**, an end-to-end encrypted messaging protocol designed for exchanging data in long-lived sessions between two devices (e.g., chats with your friends). Why is this interesting?

03 The PQC Challenge

PQC Migration and Regulation

Many mandates now exist for PQC migration:

- **NIST (US)**: Finalized PQC standards (FIPS 203–205, July 2024); vendors selling to US government must implement approved PQC.
- **White House (US)**: NSM-10 (2022) required crypto inventories & migration plans; rescinded but sustained via EO (June 2025).
- **NSA (US)**: CNSA 2.0 mandates PQC on national security systems by 2030.
- **NCSC (UK)**: Advises planning now for PQC migration in line with NIST.
- **EU (2025)**: Coordinated PQC transition roadmap (June 2025) urges Member States to inventory cryptography and complete high-risk migrations by 2030, aligning with **NIS2**, **DORA**, and **CRA**.


HITE HOUSE

MAY 04, 2022

National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems

BRIEFING ROOM › STATEMENTS AND RELEASES

NATIONAL SECURITY MEMORANDUM/NSM-10

MEMORANDUM FOR THE VICE PRESIDENT

PQC Migration and Regulation

Many mandates now exist for PQC migration from NIST, White House, *EU*, NCSC, and many others.

1. By 31.12.2026:

- At least the ***First Steps*** have been implemented by all Member States.
- Initial national PQC transition **roadmaps** have been established by all Member States.
- PQC transition **planning** and **pilots** for high- and medium-risk use cases have been initiated.

2. By 31.12.2030:

- The ***Next Steps*** have been implemented by all Member States.
- The PQC transition for **high-risk** use cases has been **completed**.
- PQC transition planning and pilots for **medium-risk** use cases have been **completed**.
- Quantum-safe software and firmware upgrades are **enabled** by default.

3. By 31.12.2035:

- The PQC transition for **medium-risk** use cases has been **completed**.
- The PQC transition for **low-risk** use cases has been **completed** as much as feasible.

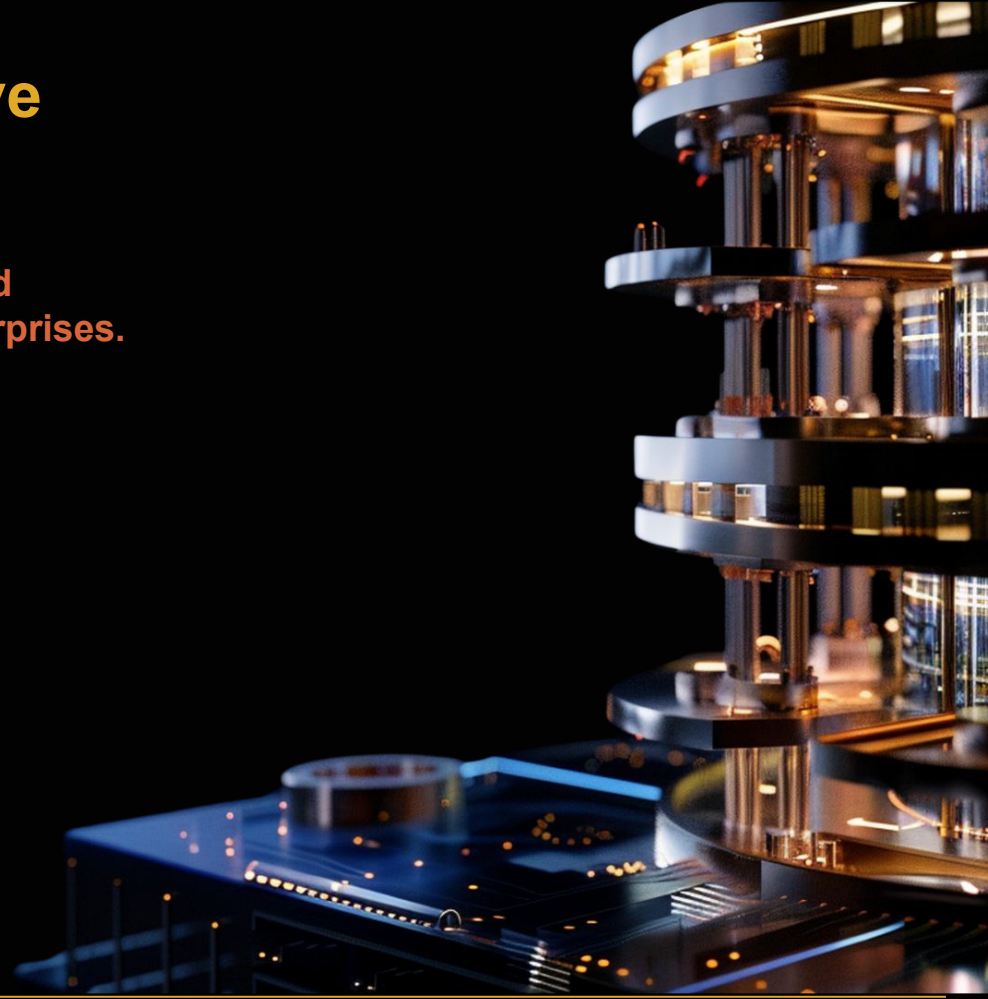
The PQC Migration Imperative

The quantum threat and the urgent need for PQC.

PQC migration

A complex, multi-faceted challenge for large enterprises.

- Vast, distributed IT environments
- Numerous legacy systems and cryptography
- Fragmented software ecosystem
- Disparate and diverse hardware



The PQC Migration Imperative

The quantum threat and the urgent need for PQC.

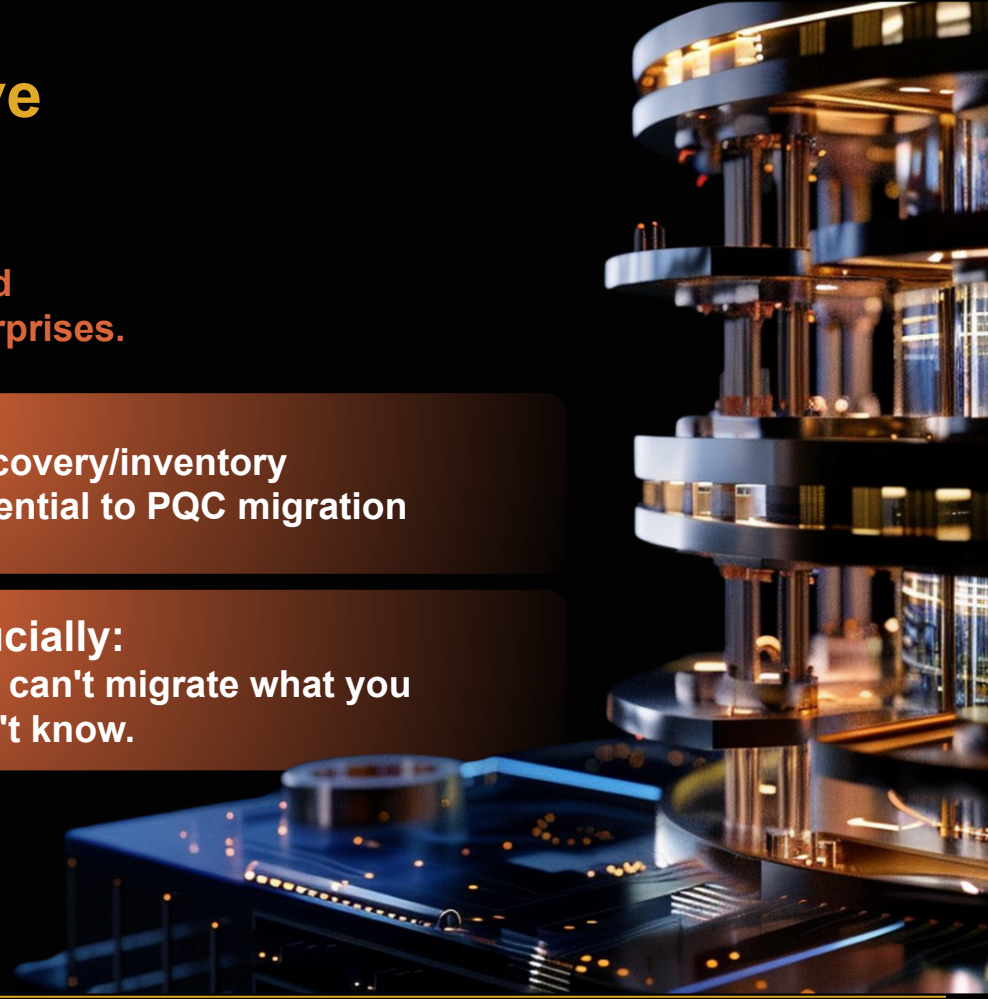
PQC migration

A complex, multi-faceted challenge for large enterprises.

- Vast, distributed IT environments
- Numerous legacy systems and cryptography
- Fragmented software ecosystem
- Disparate and diverse hardware

Discovery/inventory essential to PQC migration

Crucially:
You can't migrate what you don't know.



The Enterprise Landscape

Complexity & Fatigue

Complex IT Footprint

Vast, distributed, multi-country environments with diverse hardware and legacy systems.

Visibility Gaps

Hard to get holistic view of crypto assets & NHIs.

Tool Fatigue Burden

Enterprises are overwhelmed by siloed tools; no resources for new, non-integrated solutions.

Alert Fatigue Overload

Security teams are drowning in alerts, missing critical issues, burnout.

Cryptographic Discovery

Current Hurdles at Scale

- Traditional reliance on custom agents, scanners, and sensors.
- These offer detailed insights and 360-degree coverage.
- Enterprise-scale deployment/management presents scalability and operational issues.
- Numerous deployments demand substantial resources for installation, maintenance, and ongoing management.
- Navigating this landscape requires strategic planning for full visibility and clear PQC remediation.

Deepening Insight

Practical Integrations with Key Tools

Holistic approach
Bridges data silos for unparalleled cryptographic visibility.

Creates overall data landscape map, leveraging CMDBs and other tool insights.

Qualys.

Import certificate, secrets & TLS configs to analyze potential crypto. vulnerabilities & misconfigurations

CROWDSTRIKE

Orchestrates filesystem scanning to enable seamless scanning of remote hosts.

servicenow

Ingest certificate/asset data from its CMDB capabilities for centralized management & enhanced security posture

AWS - Key Management Service

Ingest data to enhance key management and security monitoring.

paloalto NETWORKS

Ingest and analyze TLS handshake data from Next-Generation Firewall log files.

CBOM

Cryptography Bill of Materials

Upload/analyze CBOMs for comprehensive insight.

Lessons from the Field

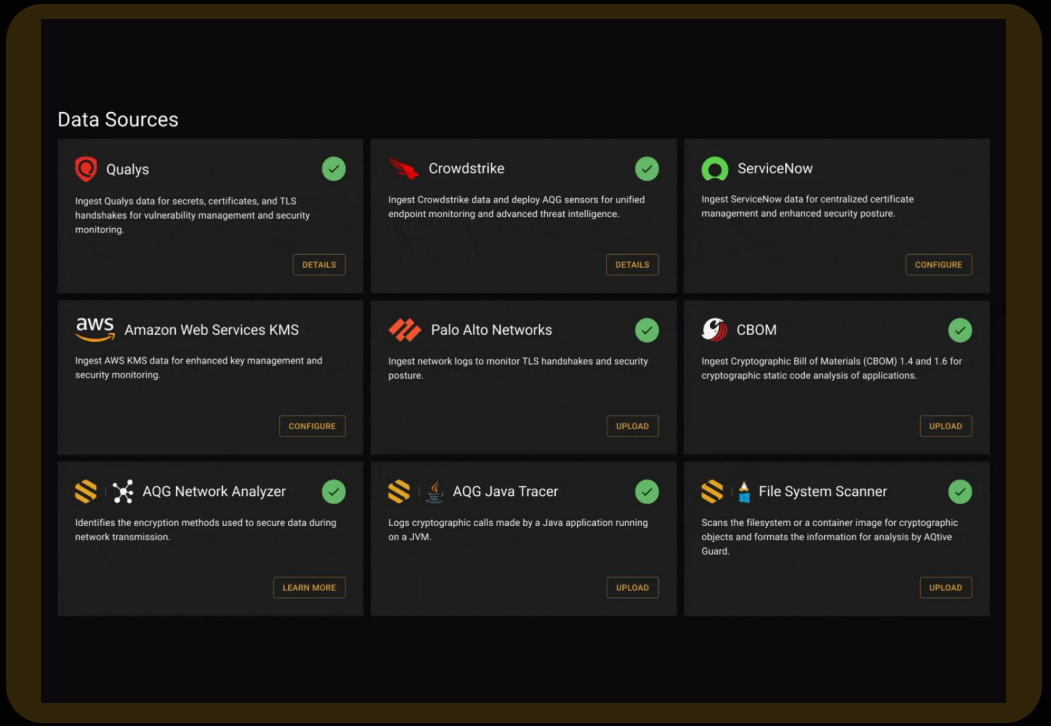
Customer-Driven Innovation

Customer feedback revealed key pain points

- High operational overhead managing numerous, siloed security agents.
- Drove the development of 3rd party ingestion for faster time-to-value, optimizing sensor deployment.
- Reduced alert fatigue via unique alerts.
- Enabled flexible asset profiling.

This feedback loop was critical for refining the solution.

Moved from "what we thought was needed" to **"what customers actually need."**

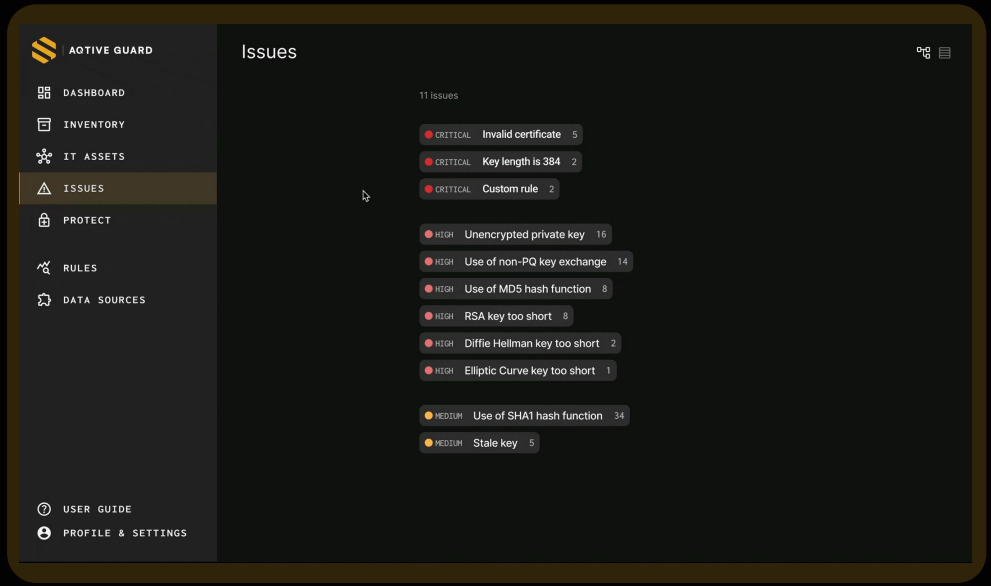


SANDBOXAQ™

Enhancing Insight

Advanced Intelligence & Actionable Filtering

- Unifies deep data from existing 3rd-party tools & first-party sensors.
- Yields actionable, meaningful data and rich context on assets and identities.
- Advanced correlation links assets to endpoints, apps, and owners for key context.
- Intelligent filtering reduces noise, delivering advanced insights with broader context.
- Deep enrichments provide rich context: '*Is this crypto mine? Do I care?*'
- Provided Knowledge graph transforms data into clear, prioritized PQC steps.



SANDBOXAQ™

Realizing Cryptographic Agility

Outcomes & Impact

Reduces Tool Fatigue
Minimizes new deployments; scales efficiently for large orgs.

Simplifies PQC Transition
Streamlines move to PQC.

Mitigates Alert Overload
Delivers prioritized, actionable insights; focuses teams on critical exposures.

Enhances Security Posture
Improves crypto agility and organizational risk readiness.

Clear Remediation Path
Guides large orgs where to start PQC migration, even with vast crypto assets.

Key Takeaways & Future Outlook

- **Smart Discovery is Key:** PQC migration success relies on intelligent discovery, not just more tools.
- **Integrate for Efficiency:** Leverage existing enterprise data and infrastructure for scale.
- **Actionable Insights:** Prioritize context and understanding over raw data volume.
- **Agile Cryptography:** Drive future readiness via intelligent system utilization.
- **Call to Action:** Engage with modern crypto and machine identity approaches.

SANDBOXAQ™

Thanks for listening!

Any questions?